UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,695	08/31/2001	Sridhar Dathathraya	SLA 1055	2135

7590 03/16/2005

David C. Ripma, Patent Counsel
Patent Counsel
Sharp Laboratories of America, Inc.
5750 NW Pacific Rim Boulevard
Camas, WA 98607

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/944,695	DATHATHRAYA, SRIDHAR	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/31/01 & 3/12/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 have been examined and is rejected under 35 U.S.C. 102(e).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Mazzagatte, et al. (US 6,862,583).

As per claim 1:

Mazzagatte, et al. discloses in a network of connected devices, a communications security method comprising:

encrypting documents with a public key; **(col.8, lines 14 and 39)**

transmitting the encrypted documents to a network-connected printer; **(col.8, line 15)**

at the printer, accepting a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

decrypting the documents with the private key; and, printing the decrypted documents. **(col.10, lines 31-39)**

As per claim 2: See col.4, lines 35-37 and col.9, lines 13-20; discussing encrypting the documents with a public key includes encrypting the documents at a network-connected computer having a public key encryption application; and, wherein transmitting the encrypted documents to a network-connected printer includes transmitting the encrypted documents from the computer, to the printer, through a network.

As per claim 3: See col.5, line 14 and col.7, line 65-col.8, line 3; discussing supplying the printer driver encryption software to the computer.

As per claim 4: See col.4, lines 54-58 and col.7, lines 33-67; discussing supplying an application to optionally encrypt documents; in response to the application, creating a graphical user interface (GUI) dialog box to invoke the document encryption option; and, in response to invoking the document encryption option, creating a graphical user interface (GUI) dialog box to request and accept public key information.

As per claim 5: See col.9, lines 13-20; discussing generating a plurality of public keys with corresponding private keys; distributing the public keys universally to network-connected computers; and, selectively distributing the private keys.

As per claim 6: See col.8, lines 32-40 and col.9, line 56; discussing the printer has a card reader to read code from SMART cards; wherein selectively

distributing the private keys includes distributing the private keys as SMART cards; and, wherein accepting a private key includes using the code read by the printer card reader.

As per claim 7: See col.4, lines 39-41 and col.10, lines 4-18; discussing storing the private keys in the printer; wherein selectively distributing the private keys includes: selectively distributing alpha-numeric codes; creating a table in the printer to cross-reference private keys with alpha-numeric codes; and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code.

As per claim 8: See col.6, line 62-col.7, line 5 and col.11, lines 17-20; discussing spooling the encrypted documents in printer memory; and, wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 9: Mazzagatte discusses the method of claim 2 further comprising:

spooling the encrypted documents to a network-connected file server; **(col.6, lines 60-65)**

notifying the printer of encrypted documents spooled on the network file server; and, **(col.10, lines 66-67)**

wherein decrypting the documents with the private key includes the printer retrieving the encrypted documents from the file server. **(col.10, lines 31-33)**

As per claim 10: See col.7, lines 13-56 and col.9, lines 26-34; discussing in response to accepting the private key, generating a list of documents encrypted with the corresponding public key; creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document; and, wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 11: See col.4, lines 37-40; discussing transmitting the encrypted documents to a network-connected printer includes transmitting a facsimile (FAX) transmission; and, wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 12:

Mazzagatte discusses the method for secure communications to a network-connected printer, the method comprising:

receiving documents encrypted with a public key; **(Col.8, lines 14 and 39)**

accepting a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

decrypting the documents with the private key; and printing the decrypted documents. **(col.10, lines 31-39)**

As per claim 13: See col.5, line 14 and col.7, line 65-col.8, line 3; discussing decrypting the documents with the private key includes operating the printer in response to publicly distributed printer driver encryption software.

As per claim 14: See col.8, lines 32-40 and col.9, line 56; discussing the printer has a card reader to read code from SMART cards; and, wherein accepting a private key includes using the code read by the printer card reader as the private key.

As per claim 15: See col.4, lines 39-41 and col.10, lines 4-18; storing the private keys in the printer; creating a table in the printer to cross-reference private keys with alpha-numeric codes; and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code as the private key.

As per claim 16: See col.6, line 62-col.7, line 5 and col.11, lines 17-20; discussing spooling the encrypted documents into a printer memory; and, wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 17: See col.7, lines 13-56 and col.9, lines 26-34; discusses in response to accepting the private key, generating a list of documents encrypted with a corresponding public key; creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document ; and, wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 18: See col.4, lines 37-40; discussing receiving documents encrypted with a public key includes receiving encrypted documents transmitted as a facsimile (FAX) transmission; and, wherein decrypting the

documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 19:

Mazzagatte discloses communications security system in a network of connected devices, the system comprising:

a computer having a network connection, an input to accept a public key, and an encryption application to supply encrypted documents to the network connection in response to accepting a public key; **(col.4, lines 40-42 and col.9, lines 13-20)**

a network connected to the computer to receive and transmit encrypted documents; and, **(col.3, lines 48-555 and col.8, lines 14-15)**

a printer having an input connected to the network to accept encrypted documents **(col.5, lines 47-50)**, the printer having an input to accept a private key corresponding to the public key used to encrypt the documents at the computer, the printer having a decryption application to decrypt the documents with the private key **(col.9, lines 13-20)**, and the printer having an output to supply a printout of the decrypted documents. **(col.10, lines 31-39)**

As per claim 20: See col.5, line 14 and col.7, line 65-col.8, line 3;

discussing the computer includes printer driver encryption software to generate the encryption application; and wherein the printer is operated in response to the printer driver encryptions software loaded in the computer.

As per claim 21: See col.4, lines 57-58 and col.7, lines 33-55; discussing the computer has a display with an input connected to the application, wherein encryption application creates a graphical user interface (GUI) dialog box on the display to optionally invoke the encryption of documents, and in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

As per claim 22: See col.7, lines 11-27; discussing a system administrator to generate a plurality of public keys with corresponding private keys, the system administrator distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

As per claim 23: See col.8, lines 32-40 and col.9, line 56; private keys configured code in SMART cards; and, wherein the printer private key input is a card reader to read SMART cards, the printer using the code read by the card reader as the private key.

As per claim 24: See col.4, lines 39-41 and col.10, lines 4-20; discussing the system administrator generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-numeric codes; and, wherein the printer private key input is a keyboard interface to accept private keys referenced by the alpha-numeric code entered on the keyboard, and the printer further comprising a memory to store the private keys, and a table to cross-reference private keys to alpha-numeric codes.

As per claim 25: See col.6, line 62-col.7, line 5 and col.11, lines 17-20; discussing the printer includes a memory to spool the encrypted documents, the printer decrypting the documents with the private key by retrieving the encrypted documents from printer memory.

As per claim 26: See col.6, lines 60-65 and col.10, lines 31-33; discussing a file server connected to the network to receive encrypted documents from the computer and to transmit encrypted documents to the printer; and, wherein the printer decrypts documents with the private key after retrieving the encrypted documents from the file server.

As per claim 27: See col.7, lines 13-67 and col.9, lines 26-34; the printer has display connected to the decryption application to depict a list of documents encrypted with a corresponding public key, in response to accepting the private key; wherein the printer decryption application creates a GUI dialog box on the display to invoke the selection of encrypted documents, the printer printing the documents in response to selecting a document from the GUI dialog box.

As per claim 28: See col.4, lines 37-40; discussing the system of claim 19 wherein the computer transmits the encrypted documents as a facsimile (FAX) transmission; wherein the network is a telephone system; and, wherein the printer decrypts the encrypted FAX transmission.

As per claim 29:

Mazzagatte discloses a secure communications network-connected printer, the printer comprising:

a network connection to receive documents encrypted with a public key; **(Col.8, lines 14 and 39)**

an input to accept a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

an decryption application to decrypt the documents with the private key; and, an output to supply a printout of the decrypted documents. **(col.10, lines 31-39)**

As per claim 30: See col.5, line 14 and col.7, line 65-col.8, line 3; discussing the decryption application is responsive to publicly distributed printer driver encryption software.

As per claim 31: See col.8, lines 32-40 and col.9, line 56; discussing the private key input is a card reader to read code from SMART cards.

As per claim 32: See col.4, lines 39-41 and col.10, lines 4-18; the private key input is a keyboard interface to accept an alpha-numeric code; and, the printer further comprising: a memory to store the private keys; a memory to store a table cross-referencing private keys with alpha-numeric codes; and, wherein private key input uses the private key referenced by the alpha-numeric code entered at the printer keyboard.

As per claim 33: See col.6, line 62-col.7, line 5 and col.11, lines 17-20; a memory to spool the encrypted documents; and, wherein decryption application retrieves the encrypted documents from printer memory for decryption.

As per claim 34: Mazzagatte discusses the printer of claim 29 further comprising:

a display having an input; **(col.9, lines 65-66)**

wherein the decryption application creates a graphical user interface (GUI) dialog box application on the display to invoke the selection of an encrypted document **(col.9, lines 63-66)**, the GUI generating a list of documents encrypted with a corresponding public key, in response to accepting the private key; and **(col.9, lines 26-34 and 10, lines 31-37)**

wherein the documents are decrypted and printed in response to the documents being selected from the GUI. **(col.7, lines 33-45)**

As per claim 35: See col.4, lines 37-40 and col.7, lines 33-45; the network connection is a telephone connection and the encrypted documents are facsimile (FAX) transmissions; and wherein the printer decrypts the encrypted FAX transmission.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100